CLEAN COPY OF AMENDED TABLE 1

Table 1

Instruction	Description	Potential Danger
Arithmetic and logical operations	A virtual machine supports the ability to add, subtract, multiply, and divide numbers and perform other common logical operations on them (*e.g.*, boolean AND, OR, etc).	Several arithmetic operations cause processor exceptions to indicate certain error conditions. For example, integer division by zero typically results in a hardware exception condition on most microprocessors.
Load operations	A virtual machine supports the ability to access memory locations associated with the instrumented program (in this case, the data address space of the operating system kernel itself).	Load operations may be misaligned, in that some microprocessors require that a 2-byte load occur on an address value that is a multiple of 2, a 4-byte load occur on an address value that is a multiple of 4, etc. If a misaligned load is attempted, the processor signals an exception. Load operations may be attempted from invalid addresses. Modern operating systems use a technique called virtual memory whereby the set of addresses associated with a user process or the operating system kernel are indirectly mapped to the physical memory addresses of the computer system. The address space of the operating system kernel is therefore sparsely populated in that not all addresses are valid and mapped to a physical memory location assigned to the operating system kernel. If a load from an address with no corresponding translation to a physical memory location is attempted, the processor signals an exception. Load operations may be attempted from addresses that are mapped to hardware devices other than memory storage and that have side effects when accessed, such as device hardware

		programmable input/output registers. Some modern operating system kernels map device control registers into the address space of the operating system so that they can be manipulated with load and store instructions. If some of these locations have side effects when loads are attempted, a sequence of loads incompatible with the mechanisms of the underlying device hardware could damage or disrupt the operation of the device or computer system itself.
Store operations	A virtual machine supports the ability to modify memory locations associated with the tracing program itself. This permits such programs to create data structures and manipulate variables.	Store operations may be misaligned in the same manner as loads and can trigger a processor exception. Store operations may be attempted to invalid locations in the same manner as loads and can trigger a processor exception. Store operations may be attempted to memory-mapped device hardware registers with side effects in the same manner as loads, resulting in damage to or disruption of a hardware device or the system. Store operations may also be attempted to a memory location that is properly aligned and valid but that is associated with a part of the operating system kernel other than the storage allocated by the virtual machine for use by the tracing program itself. If stores were permitted to such locations, tracing programs would be able to inadvertently or deliberately damage the operating system kernel.
Control transfer operations	A virtual machine supports the ability for the tracing program to direct the virtual machine to transfer control to a different point within the byte code	Control transfer instructions such as those that permit resetting the virtual machine program counter to a particular address (a "jump") and incrementing or decrementing the program counter by a particular amount (a "branch") can

	instruction stream. Such control transfer operations are required to implement standard programming constructs such as if-then statements and logical conditions.	be used to transfer control to invalid addresses, addresses that are not associated with virtual machine code, and to create programs that are non-terminating (*i.e.*, a program that loops infinitely without ever reaching a program control flow endpoint). Illegal transfers can cause exception conditions such as those enumerated for loads and stores above. Infinite loops or infinite recursion mean that program control will never return from the virtual machine to the operating system kernel, thereby utilizing the instrumentation service as a denial-of-service attack against other operating system clients.